## REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application. Applicant also thanks the Examiner for acknowledging the claim to foreign priority.

### I. Disposition of Claims

Claims 1-25 are pending in this application. Claim 1 is independent. The remaining claims depend, directly or indirectly, from claim 1. Claims 1, 13, 17, 18, 24, and 25 have been amended to correct spelling errors as requested by the Examiner. Additionally, the claims 21-25 have been renumbered as requested by the Examiner.

### II. Objection(s)

The specification and claims were objected to regarding various formalities, including spelling errors, formatting errors, and misquoted reference numerals. Accordingly, the Applicant has respectfully submitted a substitute specification. Further, the Applicant has amended the claims in view of these objections. In particular spelling errors in claims 1, 13, 17, 18, 24, and 25 have been corrected. Additionally, the numbering in claims 21-25 has been changed as requested by the Examiner. Accordingly, withdrawal of these objections are respectfully requested.

Further, Figures 12-15 and 17-19 were also objected to because they included reference numbers not mentioned in the description. The Applicant respectfully disagrees. On pages 21 and 22 of the substitute specification, reference numerals 57 and

63 of Figure 12 are disclosed. On page 21 of the substitute specification, reference numerals 55 and 60 of Figures 12-15 and 17 are disclosed. Reference numerals 175 and 52 of Figures 18 and 19, respectively, are disclosed on page 31. Further, the Examiner indicates that the SIM card is referenced by numeral 52 in the specification objections. Finally, for clarity, the specification has been amended to include the following sentence- "Like elements in the various figures will be denoted by like reference numerals for consistency." In view of the above remarks and the amendment to the specification, withdrawal to the objections of the drawings is respectfully requested.

## III. Rejection(s) under 35 U.S.C § 102

Claims 1 and 21 were rejected under 35 U.S.C. § 102(b) as being anticipated by French Patent No. 2,732,537 ("Jacques"). Claims 1-9, 10, 12, 14-18, and 21-25 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,178,242 ("Tsuria"). These rejections are respectfully traversed.

*The Present Invention*

The present invention relates to a method and apparatus for recording encrypted digital data. Figure 4 shows one or more embodiments of the present invention. In Figure 4, the present invention includes a receiver (11), *e.g.*, a satellite, an integrated receiver/decoder (or IRD) (12), a television (13) and a recording means (50), *e.g.*, a digital recorder. The recording means (50) is adapted to receive a recording support medium.

In this embodiment, the television is connected to the both the IRD (12) and the recording means (50) via a link (53, 54). Additionally, the IRD (12) and the recording

means are connected to one another via a bus (51). It is important to note that in one or more embodiments of the present invention that the IRD (12) and the recording means both include a smartcard (30, 52), respectively.

The IRD (12) receives a scrambled broadcast signal from the receiver (11). The smartcard (30) of the receiver/decoder has the ability to descramble the broadcast signal, which is then sent to the television (13). The smartcard (30) of the IRD (12), for example, as shown in Figure 5, uses various keys, which provide access to a conditional access system (21 in Figure 1) for decrypting and descrambling a scrambled broadcast signal. (See pp. 19 and 20 of the substitute specification.)

In one embodiment, the recording means (50) is adapted to decrypt and descramble the broadcast signal independent of the IRD (12) using the smartcard (52). In this embodiment, the smartcard (52) is adapted to have doubles of the keys held in the smartcard (30) of the IRD (12). In an alternative embodiment, the smartcard (30) of the IRD (12) works in the real time decryption and decoding of the broadcast signal.

As recited in claim 1, the broadcast signal (or, more generally, transmitted digital data) is encrypted by a recording encryption key. In one or more embodiments, this recording encryption key is generated by the conditional access system (21). Alternatively, the recording encryption key is generated by the smartcard (52) of the recording means (50).

In any event, the encrypted transmitted digital data is stored on a recording support medium of the recording means. Additionally, an equivalent of the recording encryption key is encrypted by another key, known as the recording transport key. The encrypted recording encryption key is also stored on the recording support medium with

the encrypted transmitted digital data. (See pp. 20-33 of the substitute specification.)

*Jacques*

In contrast, Jacques discloses a method of recording, in which a scrambled broadcast signal is forwarded by the IRD to a recording support medium in its scrambled form. A control word for descrambling the recorded, scrambled broadcast signal is encrypted using a new key. This new key is stored on the support medium and is known only to the IRD. (See p. 1 of the substitute specification.)

Clearly, Jacques does not disclose the present invention as recited in claim 1. In particular, Jacques does not disclose "that an equivalent of the recording encryption key is encrypted by a recording transport key and stored on the support medium together with the encrypted information." Jacques encrypts a control word using a new key and this new key is simply stored with the scrambled digital data. However, claim 1 requires that the recording encryption key is also encrypted by another key, namely a recording transport key, which is ultimately stored with the encrypted digital data on the recording support medium. The new key of Jacques is never encrypted.

Because Jacques does *not* disclose a new key that is encrypted by transport recording key, which is stored with encrypted, transmitted digital data on the recording support medium, Jacques cannot disclose or show the present invention as recited in claim 1. Claim 1 is patentable over Jacques. Dependent claims 2-25 are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

*Tsuria*

Tsuria also does not disclose all of the elements of the claimed invention. In

Tsuria, the digital recording system includes a IRD (11), a digital recorder (130), and a television (100). As shown in Figure 2, the scrambled digital broadcast signal (140) includes scrambled digital data segments (150, 160) and associated control messages (145, 155). Using the ECM key, a control word encapsulated in the control messages (145) is extracted. The control word is then encrypted using a transform ECM key (or TECM key). In Tsuria, after encrypting the control word using the TECM key, the scrambled digital data stream (or SDDS) is in a recording format (165). This is also clearly shown in Figure 1. The SDDS in recording format is then forwarded to the recorder for storing.

In contrast to the present invention, as recited by claim 1, Tsuria does not disclose that an equivalent of the recording encryption key is encrypted by another key, namely, a recording transport key and stored on the support medium together with the encrypted information. In particular, Tsuria does not disclose that the TECM key is encrypted by a recording transport recording key. In fact, Tsuria is completely silent to a transport recording key as required by claim 1. Consequently, Tsuria does not disclose that this transport recording key is stored with the encrypted transmitted digital data on the recording support medium.

Because the TECM key is *not* encrypted by transport recording key, which is stored with encrypted, transmitted digital data on the support medium, Tsuria cannot disclose or show the present invention as recited in claim 1. Claim 1 is patentable over Tsuria. Dependent claims 2-25 are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

## IV. Rejection(s) under 35 U.S.C § 103

Claims 11, 13, 19, and 20 were rejected under 35 U.S.C. § 103(a) as being obvious over Tsuria in view of European Patent No. 714,204 A2 ("Parks"). This rejection is respectfully traversed.

As stated above, Tsuria fails to teach all of the elements of claim 1. Parks fails to provide that which Tsuria lacks. In particular, Parks fails to teach "an equivalent of the recording encryption key is encrypted by a recording transport key and stored on the support medium together with the encrypted information," as recited in claim 1. Parks relates to a method and apparatus for processing a transmitted digital broadcast signal at a recorder. Parks is completely silent to encrypting an equivalent recording encryption key using a transport recording key and storing this encrypted key on the support medium with the encrypted, transmitted digital data.

In view of the above, Tsuria and Parks fail to show or suggest the present invention as recited in claim 1. Thus, claim 1 is patentable over Tsuria and Parks, whether considered in combination or separately. Dependent claims are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

**V. Conclusion**

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 11345.023001).

Respectfully submitted,

Date: 2/27/04

Jonathan P. Osha, Reg. No. 33,986
Rosenthal & Osha L.L.P.
One Houston Center, Suite 2800
1221 McKinney Street
Houston, TX 77010
Telephone: (713) 228-8600
Facsimile: (713) 228-8778

59640_1